COMMENTS OF SECURITYSCORECARD, INC. TO PROPOSED INTERAGENCY GUIDANCE ON THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT

PROPOSED INTERAGENCY GUIDANCE ON THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT	)))	**Docket No. OP-1752**
AGENCY NAME: BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM	))	

SecurityScorecard, Inc. (SecurityScorecard) offers comments to the proposed interagency guidance on managing risks associated with third-party relationships ("Request for Comment") jointly issued by the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Board), and the Federal Deposit Insurance Corporation (FDIC) (collectively, the agencies).[1] The agencies seek comment on the proposed guidance (the "Proposed Guidance"), the OCC's 2020 Frequently Asked Questions on Third-Party Relationships (the "2020 FAQs"), and several questions in the notice.[2] As a private sector partner offering state of the art cybersecurity ratings, including on companies operating in the financial sector, SecurityScorecard is uniquely positioned to comment on best practices to facilitate responsible and effective third-party risk management.

I. INTRODUCTION AND BACKGROUND ON SECURITYSCORECARD

SecurityScorecard is an industry-leading security ratings platform backed by, amongst other investors, Google Ventures (GV), Riverwood Capital, Silver Lake Waterman, and Fitch Ventures. SecurityScorecard's A-F ratings system helps companies understand, improve, and communicate their own and their third parties' cybersecurity risk to management, directors, investors, employees, insurers, and, increasingly, regulators. SecurityScorecard's platform is used by more than 23,000 organizations worldwide, including at least 100 of the Fortune 500, top payment processors, and major national and

[1] The Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation, *Proposed Interagency Guidance on Third-Party Relationships: Risk Management, Request for Comment*, Section III.

[2] *Id.* at Text of Proposed Guidance on Third-Party Relationships, Section IV; *Id.* at OCC's 2020 Frequently Asked Questions (FAQs) on Third-Party Relationships, Section V.

foreign financial institutions. SecurityScorecard's data is also used by supply chain risk management programs in State and local governments across the United States, and the FDIC.

Generated using only publicly-available indicators, SecurityScorecard's ratings measure an entity's cyber-hygiene across ten risk categories:

1. NETWORK SECURITY (detecting insecure network settings);
2. DNS HEALTH (detecting insecure configurations and vulnerabilities);
3. PATCHING CADENCE (detecting out-of-date company assets which may contain vulnerabilities or risks);
4. ENDPOINT SECURITY (measuring security level of employee workstations);
5. IP REPUTATION (detecting suspicious activity, such as malware or spam, within a company network);
6. APPLICATION SECURITY (detecting common website application vulnerabilities);
7. CUBIT SCORE (proprietary algorithms checking for implementation of common security best practices);
8. HACKER CHATTER (monitoring hacker sites for chatter about your company);
9. INFORMATION LEAK (detecting potentially confidential company information which may have been inadvertently leaked); and
10. SOCIAL ENGINEERING (measuring company awareness to a social engineering or phishing attack).

SecurityScorecard automatically scans the entire internet daily, updating each organization's potential vulnerabilities and monitoring for new threats every 24 hours. This continuous monitoring helps alert entities to previously unknown exposures specific to them, their supply chain and their vendors, and importantly, provides a dynamic assessment of a company's security posture, as opposed to a traditional, point-in-time one. In this way, SecurityScorecard's security ratings help assess and mitigate cyber risks to prevent a material disruption of a banking organization's operations and the American financial sector more broadly, and facilitate the ability of both banking organizations and bank service providers to comply with

the proposed rule addressing Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, jointly published by the agencies in January 2021. This proposed rule would, in pertinent part, require prompt notification of a qualifying incident to their respective regulators (no later than 36 hours). Moreover, such proposal imposes specific obligations upon bank service providers to notify affected banking organization customers immediately after the bank service provider experiences a computer security incident that it believes in good faith could disrupt, degrade, or impair services provided to a banking organization for four or more hours.[3]

SecurityScorecard agrees that a uniform framework on managing third-party relationships in the financial services sector is needed and posits that achieving sound risk management practices identified in the Proposed Guidance, at least in the cyber context, will be significantly strengthened by dynamic, real-time security ratings. While the utility of continuously-monitored security ratings is most evident in three stages of the third-party risk management life cycle (due diligence and third-party selection, ongoing monitoring, and contract negotiation), each of which is addressed in the comments below, leading security ratings platforms such as SecurityScorecard can also help the agencies advise regulated entities on issues of cybersecurity, track in virtually real-time the cyberhealth of key technology and bank service providers involved in critical activities, and aid in investigations of agency-regulated entities that have experienced a computer-security incident or notification incident.

II. SECURITYSCORECARD IDENTIFIES THE FOLLOWING AREAS OF THE PROPOSED GUIDANCE AND 2020 FAQS TO FACILITATE RESPONSIBLE PROCUREMENT PRACTICES FOR BANKING ORGANIZATIONS

A. Security Ratings are an Effective Tool for Both Established and Smaller Banking Organizations to Reduce Risk and Achieve Economies of Scale in the Cyber Diligence Context

While cybersecurity diligence is an integral part of standard procurement processes, most entities obtaining third party services lack the capacity or a standardized framework within which to meaningfully

[3] Federal Register, Vol. 86, No. 7, Proposed Rules, "*Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*", RIN (1557–AF02 (OCC), 7100–AF (Board), 3064–AF59 (FDIC), January 12, 2021, available online at: https://www.fdic.gov/news/board/2020/2020-12-15-notice-sum-c-fr.pdf.

evaluate cyber risk of their many vendors, posing a security risk to the American financial ecosystem. This risk is exacerbated by the tremendous degree to which critical bank functions or activities are outsourced and the myriad business arrangements that qualify as third-party relationships.

***"How could the proposed guidance better help a banking organization appropriately scale its third-party risk management practices?" Request for Comment*, Section C.6.**

SecurityScorecard encourages the agencies to emphasize the importance of security ratings and continuous, non-intrusive monitoring in the Proposed Guidance as an effective tool to both (1) reduce risk in the diligence process, and (2) appropriately scale third-party risk management practices. First, access to a third party's real-time security score is a powerful point of reference during the due diligence and third-party selection stage. Beyond reviewing, as recommended by the Proposed Guidance, where available, a System and Organization Control (SOC) report or other independent third-party assessment (which offers a static point of reference that, at time of third-party selection, may already be outdated), access to a real-time assessment of a third party's internal controls and information security program is both more informative and responsive to the negotiation in progress. *Proposed Guidance*, Section C.2.g. This can help banking organizations more accurately evaluate and reduce the associated risk.

Further, during the negotiation stage, security scores provide an intrinsic means for a banking organization to audit a third-party at the outset of, and throughout, a business relationship, independent of such third party's discretion of whether, when, and in what form to proffer a security assessment to their counterparty. Availability of security ratings can be used to support a banking organization's right to audit and require remediation by taking the nature of auditing beyond the periodic reports contemplated by the Proposed Guidance, and divorcing it from having to align with a banking organization's in-house capacity to monitor performance with the contract. *Proposed Guidance*, Section C.3.d. After all, on a security ratings platform, a banking organization need not deploy significantly more resources to evaluate the security posture of one vendor versus dozens. With security ratings at hand, contractual auditing through a security

lens can be easily implemented by banking organizations.

Second, as it concerns ongoing monitoring, security ratings allow businesses to achieve economies of scale by standardizing the diligence process and continuously monitoring bank service providers' cybersecurity posture on their behalf. Endorsement or recommendation of banking organizations adopting the use of security ratings in the Proposed Guidance would help alleviate the concern expressed by "[s]ome smaller and less complex banking organizations […] that they are expected to institute third-party risk management practices that they perceive to be more appropriate for larger and more complex banking organizations." *Request for Comment*, Section C. Security ratings would easily provide smaller banking organizations with reliable, real-time security indicators that do not require significant resource investment. In fact, in keeping with its mission to make the cyber world a safer place, SecurityScorecard provides any company with its own score for free. Likewise, per the concern expressed by certain third-parties in FAQ No. 17 ("*Some third parties, such as fintechs, start-ups, and small businesses, are often limited in their ability to provide the same level of due diligence-related information as larger or more established third parties*"), security ratings allow entities with limited resources to point to objective metrics] during the diligence process, similar to what larger or established banking organizations use during the same. *2020 FAQs*, No. 17. This proposal is consistent with several key regulatory standards, such as the Bank Secrecy Act (BSA), with which many of those same entities need comply, and which already require them to conduct cybersecurity evaluations and to prepare cybersecurity incident response plans—for example, as part of their BSA audit assessments. Security ratings are a natural part of that process.

The agencies' endorsement of security ratings also would have them join the ranks of various other stakeholders that have already publicly supported security ratings as an effective tool to mitigate cybersecurity risks across American critical infrastructure, including in the financial services sector:

i. The Cybersecurity and Infrastructure Security Agency (CISA) National Risk Management Center recently launched a new cyber venture called System Cyber Risk Reduction,

explicitly highlighting the utility of security ratings as a valuable metric of cyber risk.[4] A blog authored by CISA's Assistant Director for the National Risk Management Center states:

> "*The emergence of security ratings has driven cyber risk quantification as a way to calculate and measure cyber risk exposure. These security ratings provide a starting point for companies' cybersecurity capabilities and help elevate cyber risk to board decision making. Entities can also use security ratings alongside strategic risk metrics to align cyber scenarios with material business exposure; rollup cyber risks with financial exposure to inform risk management decisions; and measure improvement of cyber risk reduction over time. This kind of work needs to happen in the boardroom and also amongst national security leaders*."[5]

CISA's endorsement of security ratings calls important attention to how ratings have emerged as an industry-standard best practice.

ii. On May 12, 2021, U.S. President Joseph Biden issued his *Executive Order on Improving the Nation's Cybersecurity*. Section 4 of the order addresses the Federal Government's efforts to enhance software supply chain security, including by requiring that the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology (NIST), in coordination with the Chair of the Federal Trade Commission, to "identify secure software development practices or criteria for a consumer software labeling program […] [to] identify, modify, or develop a recommended label, or, if practicable, a tiered software security rating system [that] shall focus on ease of use for

[4] B. Kolasky, *A Risk-Based Approach to National Cybersecurity*, CISA blog (January 14, 2021), available online at: https://www.cisa.gov/blog/2021/01/14/risk-based-approach-national-cybersecurity.
[5] *Id.*

consumers and […] maximize participation."[6] The order is compelling legitimization of security ratings as a key to enhancing supply chain security.[7]

iii. The Cybersecurity Solarium Commission recommended last year that Congress establish and fund a National Cybersecurity Certification and Labeling Authority, similar to Energy Star appliance ratings.[8]

iv. The U.S. Chamber of Commerce described in 2017 the potential of "reliable security ratings that are fair, accurate, and clear [to] enhance security across the economy."[9] In conjunction with security ratings companies, the Chamber also developed a concrete set of principles on which to generate cybersecurity scores.[10]

B. The Proposed Guidance should identify reputable cybersecurity metrics as a valid means to supplement a banking organization's information security due diligence

In addressing FAQ No. 5 *("What type of due diligence and ongoing monitoring should be conducted when a bank enters into a contractual arrangement in which the bank has limited negotiating power?")*, the OCC recommends that "bank management [] take appropriate actions to manage the risks" in contractual arrangements in which the bank has limited negotiating power, including "determining appropriate alternative methods to analyze these critical third parties (e.g., use information posted on the third party's website)." *2020 FAQs*, No. 5. This concept merits inclusion in the Proposed Guidance, and should be strengthened with the example of continuously updated security ratings as an appropriate alternative method to diligence a critical third party. Likewise, the Proposed Guidance should identify

[6] The White House, *Executive Order on Improving the Nation's Cybersecurity*, May 12, 2021, available online at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.
[7] *Id.*
[8] United States of America Cyberspace Solarium Commission, *March 2020 Final Report*, available at: https://perma.cc/8KC8-XHN4.
[9] A. Beauchesne, *Why We Need Fair and Accurate Cybersecurity Ratings,* U.S. Chamber of Commerce (June 20, 2017, 9:00 AM), available online at: https://www.uschamber.com/series/above-the-fold/why-we-need-fair-and-accurate-cybersecurity-ratings.
[10] U.S. Chamber of Commerce, *Principles for Fair and Accurate Security Ratings*, (June 20, 2017, 10:00 AM), available online at: https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings.

reputable cybersecurity metrics as an acceptable mitigating factor where "a banking organization may not be able to obtain the desired due diligence information from the third party," since ratings such as those generated by SecurityScorecard draw from publicly-available indicators whose accuracy and completeness are not conditioned on any company's decision to provide or withhold important information. *Proposed Guidance*, Section C.2. In particular where the third party has provided limited diligence information, taking into account a third party's security ratings would afford banking organizations supervised by all three agencies increased negotiating power as it regards information security; management of information systems; and operational resilience. *Proposed Guidance*, Section C.2(h) – (j).

> "***What additional information should the proposed guidance provide regarding a banking organization's assessment of a third party's information security and regarding information security risks involved with engaging a third party?*" *Request for Comment*, Section G.17.**

The efficiencies of security ratings have important implications for both the third and fifth stages of the third-party risk management life cycle (contract negotiation and ongoing monitoring, respectively), which the Proposed Guidance should identify. As it concerns contract negotiation, and more specifically performance measures or benchmarks, the Proposed Guidance contemplates service-level agreements between banking organizations and third parties that "specif[y] measures surrounding the expectations and responsibilities for both parties, including conformance with regulatory standards or rules." *Proposed Guidance*, Section C.3b. SecurityScorecard encourages the agencies to consider incorporating security ratings into this concept by promoting contractual arrangements with only third parties that have achieved a minimum acceptable score and that contractually agree to maintain at least such score for the full term of the contract. Such minimum score will vary across third parties, and should reflect the risk profile and complexity of the third-party relationship, taking into account the same factors contemplated in the Proposed Guidance, including the level of access a third party is granted to a banking organization's systems or sensitive data and whether the third-party relationship would support critical activities. That is to say, a

higher minimum acceptable score would be expected of bank service providers that present a significant risk to the banking organization. With this said, companies must keep in mind that even perceived low-risk third party vendors could pose an outsized risk—for example, in 2014, a large merchandise retailer experienced a cyber-intrusion that was traced back to stolen network credentials the retailer had granted to its refrigeration and heating, ventilation, and air conditioning (HVAC) systems vendor. In line with the Proposed Guidance, a minimum performance measure would "not incentivize undesirable performance or behavior, such as encouraging processing volume or speed without regard for timeliness, accuracy, compliance requirements, or adverse effects on banking organization customers," but rather reward those that prioritize security in their procurement processes. *Proposed Guidance*, Section C.3b.

Further to the discussion above, a minimum performance measure would help regulated entities verify third parties' point-in-time information security claims at the outset of and throughout the business arrangement. The agencies might also consider a security ratings "safe harbor" in connection with third party notification incidents. For example, the agencies could pledge that regulated banking organizations that made a procurement decision in reliance on a third party's qualifying score as issued by an agency-authorized security ratings platform will not be the subject of a related enforcement action, provided they monitor that third party and ensure maintenance of an acceptable score throughout the period of performance.

Insofar as it concerns ongoing monitoring, the Proposed Guidance acknowledges that "the appropriate degree of ongoing monitoring is commensurate with the level of risk and complexity of the third-party relationship." *Proposed Guidance*, Section C.5. While true, security ratings such as those offered by SecurityScorecard allow banking organizations of all sizes and complexity to apply rigorous, ongoing monitoring to all vendors across the risk spectrum, alleviating the burden of articulating the precise degree of oversight that is warranted in any given business arrangement. Smaller banking organizations need no longer dispense limited resources on periodically evaluating the security posture of its highest-risk vendors when they can leverage security ratings to monitor all vendors in a similar manner at a reasonable cost. Continuous ratings allow banking organizations to assume a defensive approach to cyber risk, which

can produce tremendous downstream protection for banking organizations and the American financial sector more broadly.

III. CONCLUSION

SecurityScorecard respectfully requests that the agencies consider the foregoing comments in respect of the Proposed Guidance and 2020 FAQs.

Respectfully submitted,

Charlie Moskowitz
Vice President, Policy and Government Affairs
SecurityScorecard

September 17, 2021